ESTELLE SPECIFICATION OF MIL-STD-188-220A DATALINK LAYER

Paul D. Amer   R. Gregory Burch, Jr.
Adarshpal Sethi   Dong Zhu
University of Delaware
Newark, DE 19716

Ted Dzik
Raymond Menell
US Army CECOM
Fort Monmouth, NJ 07703

Mike McMahon
ARINC, Inc.
Shrewsbury, NJ 07702

Abstract

This paper presents ongoing results of a contract between US Army CECOM and the University of Delaware to develop a formal specification of the datalink layer of MIL-STD-188-220A using the ISO International Standard Formal Description Technique Estelle (ISO 9074). The Estelle specification aims at discovering and resolving ambiguities in the original English document that would cause interpretation problems for implementors. The proposed architecture closely models ISO 8802's Logical Link Control for local area networks [7]. The paper also presents the state tables and transitions which constitute the modules of this architecture. At MILCOM 95, we reported on our initial effort to specify an earlier version titled 188-220 (version 7 May 1993) with support from the Army Research Laboratory in Aberdeen Proving Ground, MD [6]. Several updates have been generated since then as a result of regular meetings of the Combat Net Radio (CNR) Implementation Working Group (WG), previously known as the MIL-STD-188-220 WG. Our current specification efforts are based on the most recent version dated 27 Jul 1995. Thus far, over 30 ambiguities or inconsistencies (some minor, some major) have been discovered and reported to the CNR working group for incorporation into the developing 188-220A standard.

1 Introduction

MIL-STD-188-220 was originally a joint services interoperability standard for digital message transfer device subsystems [3]. MIL-STD-188-220A has evolved to become the standard for interoperability of command, control, communications, computers, and intelligence (C^4I) systems over Combat Net Radio (CNR) [4]. It is a key component of the Army Technical Architecture (ATA) for the digitized battlefield, and will likely become so in the Joint Technical Architecture (JTA). There are several synergistic efforts to assure that the standard is complete, correct, unambiguous, and performing suitably well. To ensure that the 188-220A standard is free from ambiguities which might cause implementation problems, we have used the Estelle language, an ISO International Standard formal description technique (FDT), to create an unambiguous specification of the 27 Jul 95 version of the standard [1,2].

Delaware's specification effort is divided into three subprojects: specifying Type 1: Connectionless (CL) Operation (unacknowledged and coupled acknowledged); specifying Type 2: Connection-mode Operation; and specifying Type 4: Decoupled Acknowledged Connectionless Operation.[1]

Our specfications in Estelle are based upon a modular architecture where each module represents a different component of the datalink layer of 188-220A. Each module's proposed behavior is formally specified as an extended finite state machine (EFSM). These EFSMs then communicate with each other via interactions as semantically defined in the Estelle ISO standard. It is our hope that our continuing development of these specifications will further contribute to the correctness of MIL-STD-188-220A as it continues to evolve.

The paper is organized as follows. Section 2 gives an overview of MIL-STD-188-220A, focusing on the part most relevant to our work, i.e., the link layer. Section 3 presents several different aspects of the specification work itself. First, this section provides the general architectures for Type 1 and Type 4 services[2], and demonstrates the hierarchical nature of Estelle specfications. Next the section presents some typical state diagrams and a state transition table which constitute the modules in these architectures. Finally, the section also includes a discussion of typical exam-

This work supported, in part, by the US Army Research Office Scientific Services Program administered by Battelle (DAAL03-91-C-0034), by the US Army Research Office (DAAL03-91-G-0086, DAAL03-92-G-0070), and by the U.S. Department of the Army, Army Research Laboratory under Cooperative Agreement DAAL01-96-2-0002 Federated Laboratory ATIRP Consortium.

[1] Type 3 Connectionless Acknowledged Operation is considered part of Type 1.

[2] The Type 2 Service architecture and specification are currently being developed.

Figure 1: General Architecture

3.1 Link Layer Service Architectures

MIL-STD-188-220A specifies several different service types, each intended to handle different types of traffic with different quality of service (QOS) demands. In developing the formal Estelle specification, we have modularized these different services into separate architectures which show the different Estelle components needed to achieve these services. A 188-220A station can actually process several different types of traffic simultaneously (and almost orthogonally). Consider a station which is equipped to handle both Type 1 and Type 4 traffic; such a station has an organization as represented by the architecture in Figure 2. As an example of how this architecture models data flow in a station, consider the Network Layer sending a DL_Unitdata_Request with low reliability. According to the standard's QOS mappings, this request should be serviced as a Type 1 unacknowledged transmission. When this interaction enters the Station Component through the interaction point labeled "LSAP", the Station Component determines the correct handling of the request and forwards it to the "Type 1 Service" box. This box generates the UI (Unnumbered Information) PDU and forwards it to the Station Component, which will eventually forward it to the physical layer through the interaction point labeled "PSAP".

Figure 3 shows the Type 1 Service architecture. Because Type 1 Service includes acknowledgments, this architecture includes acknowledgment timers as dic-

Figure 4: Architecture for Type 4 Service

definition is achieved through the creation of communicating extended finite state machines on which Estelle is based. Once all states and transitions (including inputs and outputs) are finalized, the writing of the Estelle code itself is straightforward.

Figure 5 is an example of a state diagram for one of these machines. This particular diagram shows the operation of a station in its Initialization Phase, which itself is part of the state machine of the Station Component (see Figure 2). Every combination of in-

Figure 5: State Diagram for Initialization Phase

put and current state results in a transition to some specified state; as such, the possibility of ambiguity is eliminated. The full range of possible state/input combinations results in a state transition table for this ESFM as shown in Figure 6. The majority of ambiguities discovered in the 188-220A document was found as a result of trying to formulate these state tables from the English text.

3.3 Summary of Problems and Ambiguities

The primary goal in developing an Estelle formal specification is to discover and document problems and ambiguities that are commonly seen in a standard written in natural language. In the process of developing the specifications, we have documented more than thirty problems and ambiguities in the original English document. These problems have been reported to the Working Group and, in many cases, have resulted in changes and rewordings of the standard. Here we present a representative cross-section of examples of ambiguities found, demonstrating the difficulty of defining protocol operations in a natural language.

- The following statement is taken directly from the 27 Jul 1995 draft of the standard, Section 5.3.7.2.5.2, item b(2): "a station shall ... wait for some period of time bounded by the probability of the remote acknowledgment time expiration...." This sentence is unclear: how can a time period be bounded by a probability? The WG has acknowledged the ambiguity of this section at the 13 Mar meeting and is currently working on a specific rewriting.
- The standard indicates in Section 5.3.8.1.2.e that *k* is a link parameter defined to be the "maximum number of outstanding I PDU's." But in Section 5.3.7.2.5.1, we see that the "...RR command is sent to a destination station when the *k* value at the originating station reaches half of the *k* value for that connection." In Section 5.3.7.2.5.1, the first reference to *k* indicates that *k* is a variable which is being used as a counter, while the second reference to *k* has *k* being a static parameter for that connection. In this case, the standard was changed such that the variable counting the number of outstanding I PDUs was not referred to as *k*.
- In Section 5.3.6.1.9, the standard indicates that "the URNR response PDU shall be used to reply to a UI command PDU with the P-bit set to 1, if the UI command cannot be processed due to a busy condition." Since the UI cannot be processed, this indicates the URNR does *not* acknowledge the UI. However, Section 5.3.5.2.3.2 states that "the F-bit set to 1 shall be used to acknowledge the receipt of a command PDU with the P-bit set to 1." And Section 5.3.7.1.5.4 indicates that "a URNR response PDU, with F-bit set to 1, may be sent by the remote station to advise the originator of the associated UI command PDU that it is experiencing a busy condition and is unable to accept UI PDU's." The combination of the last two excerpts implies that URNR response PDU's *do* acknowledge the corresponding UI PDU. A correction of this contradiction was approved at the 13 Mar 96 WG meeting. Section 5.3.5.2.3.2 was changed to read "the F-bit set to 1 shall be used to *respond* to the receipt of a command PDU with P-bit set to 1." No acknowledgment is implied.
- In Section 5.3.16, the DL_Status_Indication "Acknowledgment Failure" was originally defined with no explanation of how upper layers are to know *which* DL_Unitdata_Requests failed. We suggested that an identification field is needed to correlate Failure indications with the appropriate DL_Unitdata_Requests, and this suggestion has been incorporated into the standard.
- In Section 5.3.3.1.2, the standard states that "For efficiency at system startup, connections may be

Figure 6: State Transition Table for Initialization Phase

assumed to exist with all other stations in the network...." We have suggested adding text to help implementors understand exactly what this sentence means in the context of the protocol mechanisms which actually provide the connection-oriented service.

- Section 5.3.7.2.5.4.2 states that "When an I PDU has been received and not more than one frame is missing, the station may retain the information field of the out-of-sequence I PDUs and send a SREJ PDU for the missing I PDU." This sentence implies at most one missing I PDU when sending an SREJ PDU. The next sentence, however, states "A station may transmit one or more SREJ PDUs, each containing a different N(R) with P-bit set to 0." This sentence implies that there can be more than one missing I PDU (otherwise why send multiple SREJ PDUs with different N(R)?). At the 13 Mar meeting, the WG changed this section to indicate that an SREJ PDU may be sent when *at least one*, rather than "no more than one," I PDU is detected as missing.

These examples show the difficulties of describing protocol operations with clarity, precision, and consistency, using a natural language. Ambiguities and contradictions frequently arise when related protocol functionalities are described in different document sections separated by pages of unrelated text. Such problems are eliminated in a formal Estelle specification. All actions in a particular context must be defined in one place within the Estelle specification. The specifications make the conditions for state transitions explicit through Estelle constructs. Indeed, the very process of creating these constructs enables formal specifiers to detect some of these types of ambiguities which are difficult to see in normal reading.

4 Conclusion

The Army has embarked upon a program for digitizing the battlefield to meet the challenges of the 21st century. The goal is to ensure command and control superiority by providing warfighters with a horizontally and vertically integrated digital information network via more sophistocated tactical C^{4}I systems at lower echelons to provide a consistent picture of the battlefield from soldier to commander. To this end, we have presented an Estelle specification of the MIL-STD-188-220A Datalink Layer. This effort has enabled the Working Group and implementors to resolve some of the ambiguities in the original English document, leading to interoperable implementations of the protocol. As our work continues with the CNR Working Group, we hope that the specification effort will further contribute to the correctness of MIL-STD-188-220A, resulting C^{4}I system developments, and the capabilities needed by the warfighter.

5 References

[1] S. Budkowski, P. Dembinski. "An Introduction to Estelle: A Specification Language for Distributed Systems," *Computer Networks and ISDN Systems*, 14(1), 1987, 3-24.

[2] Information Processing Systems – Open Systems Interconnection: Estelle, A Formal Description Technique Based on Extended State Transition Model, ISO International Standard 9074, June 1989.

[3] Military Standard – Interoperability Standard for Digital Message Transfer Device Subsystems (MIL-STD-188-220), 7 May 1993.

[4] Military Standard – Interoperability Standard for Digital Message Transfer Device Subsystems (MIL-STD-188-220A), 27 Jul 1995.

[5] J. Siliato, J. Lathan. "Combat Net Radio (CNR) Protocols: A Means for Battlefield Digitization", Tech Report, U.S. Army Communications-Electronics Command, 16 November 1993.

[6] H. Li, P. Amer, S. Chamberlain. "Estelle Specification of MIL-STD-188-220 Datalink Layer Interoperability Standard for Digital Message Transfer Device Subsystems," *Proceedings of MILCOM '95*, November 1995.

[7] Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – ISO International Standard 8802-2, December, 1994.